REMARKS

Applicant submits that the present supplemental amendment should be considered as supplemental to and part of the amendment filed on December 22, 2008, and both amendments are fully responsive to the Office Action dated June 20, 2008 and, thus, the application is in condition for allowance.

By this reply, claim 37 is amended. Claims 37-40 remain pending. Of these, claim 37 is independent. An expedited review and allowance of the application is respectfully requested.

In the outstanding Office Action, claims 37-40 were rejected under 35 U.S.C. § 102(e) as being anticipated by Rezaiifar (USPN 6,980,658) as evidenced by Lin (IS-95 North American Standard – A CDMA Based Digital Cellular System). It is asserted that Rezaiifar discloses a method with all of the limitations of the present invention as recited in the claims. Applicant respectfully traverses.

Rezaiifar cannot anticipate the present invention as recited in the pending claims because Rezaiifar does not teach or fairly suggest each of the elements recited therein. For example, Rezaiifar does not disclose or suggest a method including the steps of decrypting a data packet containing a checksum and a payload, the checksum included in a header of the data packet and based upon the payload, the decrypting accomplished using a forward cipher key; and calculating a calculated checksum for the data packet, the calculated checksum generated by a checksum generator based on the payload of the data packet. Rezaiifar discloses a method for encrypting transmissions (Rezaiifar, Column 2, Lines 18-23). At best Rezaiifar discloses a method for transmitting authentication variables. See, for example, claim 1. At no point does Rezaiifar disclose a method wherein a checksum is included within the header of a data packet. A checksum is a fixed-size datum computed from an arbitrary block of digital data for the purpose

of detecting accidental errors that may have been introduced during its transmissions or storage. The checksum is included within the header of a data packet, for example, in order to minimize the bandwidth necessary to detect a loss of synchronization. The checksum is created based upon the payload being sent such that it can be compared to a calculated checksum of the payload received. This, for instance, allows the method to determine if an encryption key stream and a decryption key stream remain synchronized. However, Rezaiifar does not contain any such element. The method of Rezaiifar is a completely different way of authenticating. Rezaiifar states that an individual crypto-sync value is determined for each data unit that is to be encrypted and each crypto-sync value results in a different cipher-text even for the same clear-text (Rezaiifar, Column 6, Lines 41-44). The crypto-sync is thus very different from the checksum in the present invention. For example, in the present invention, if a checksum value results in a different cipher-text even for the same clear-text, there is no way the calculated checksum would be able to match with the checksum. The methods of Rezaiifar and the present invention are thus incompatible. Thus, Rezaiifar cannot anticipate the present claim. Therefore, the rejection should be withdrawn and the application allowed to proceed to issue.

Rezaiifar does not teach all of the elements in the independent claim. Hence, the dependent claims, which depend therefrom, also are patentably distinct from Rezaiifar. For this reason, Applicant respectfully requests withdrawal of the rejection.

In the outstanding Office Action, claims 37-40 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Lockhart (USPN 5,841,873) in view of Menezes ("Handbook of Applied Cryptography"). It is asserted that Lockhart discloses a method and system with all of the limitations of the present invention as recited in the claims, but for the encryption algorithm being a stream cipher. It is further alleged that Menezes does disclose this deficiency and the

combination of these cited references would have therefore been obvious to one having ordinary skill in the art. Applicant respectfully traverses.

Neither Lockhart, nor Menezes, nor any other related art of record, alone or in combination, disclose or fairly suggest the present invention as recited in the pending claims. For example, none of the related art recites a method including the steps of decrypting a data packet containing a checksum and a payload, the checksum included in a header of the data packet and based upon the payload, the decrypting accomplished using a forward cipher key; and calculating a calculated checksum for the data packet, the calculated checksum generated by a checksum generator based on the payload of the data packet. Lockhart discloses a method of detecting encryption errors (Lockhart, Column 2, Lines 58-61). Nowhere does Lockhart disclose including a checksum within the header of a data packet. This, for example, minimizes the bandwidth necessary to detect a loss of synchronization. As stated above, the checksum is created based upon the payload being sent such that it can be compared to a calculated checksum of the payload received. Lockhart does not even disclose a checksum, neither one in the header nor one calculated from the payload. This element is simply not present. Therefore, even with the combination of Menezes, Lockhart cannot anticipate or obviate the present invention. Furthermore, there is no specific motivation disclosed or suggested in the cited art, other than Applicant's own disclosure, that would motivate one having ordinary skill in the art to create the invention as recited in the pending claims. The Office Action has used improper hindsight reconstruction to attempt to re-create Applicant's own invention using selected parts of various references. When taken as a whole, however, the references could not be fairly combined to create the invention as recited in the pending claims. For at least this reason, the rejection should be withdrawn.

Because neither Lockhart nor Menezes, alone or in combination, teach all of the elements in the independent claim, the dependent claims, which depend therefrom, also are patentably distinct from any prior art of record. For this reason, Applicant respectfully requests withdrawal of the rejection. Furthermore, there is no motivation to combine any of these references outside of Applicant's own disclosure. Even if they were combinable, *arguendo*, the combination would not be able to obviate the present invention for at least the reasons set forth above. Thus, the rejection of the claims should be withdrawn.

No fees are believed necessary to enter this amendment. If any fees are associated with the entering and consideration of this amendment, please charge such fees to our Deposit Account 50-2882.

Applicant respectfully requests an interview with the Examiner to present more evidence of the unique attributes of the present invention in person. As all of the outstanding rejections have been traversed and all of the claims are believed to be in condition for allowance, Applicant respectfully requests issuance of a Notice of Allowance. If the undersigned attorney can assist in any matters regarding examination of this application, Examiner is encouraged to call at the number listed below.

Respectfully submitted,

Date: March 12, 2009

/Fariborz Moazzam, Reg. No. 53,339/

Fariborz Moazzam
Reg. No. 53,339
Cust. No. 39,013

MOAZZAM & ASSOCIATES, LLC
7601 Lewinsville Road, Suite 304
McLean, Virginia 22102
(703) 442-9480; (703) 991-5978 (fax)